

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
 United States Patent and Trademark
 Office
 Box PCT
 Washington, D.C. 20231
 ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 12 April 2000 (12.04.00)	
International application No. PCT/IB99/01494	Applicant's or agent's file reference SZ9-98-004
International filing date (day/month/year) 02 September 1999 (02.09.99)	Priority date (day/month/year) 21 September 1998 (21.09.98)
Applicant ABAD PEIRO, Jose L. et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

11 March 2000 (11.03.00)

☐ in a notice effecting later election filed with the International Bureau on:2. The election ☒ was☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer S. Mafla
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference SZ9-98-004	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/IB 99/ 01494	International filing date (day/month/year) 02/09/1999	(Earliest) Priority Date (day/month/year) 21/09/1998
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

- a. With regard to the language, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international search was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

2. ☐ Certain claims were found unsearchable (See Box I).

3. ☐ Unity of invention is lacking (see Box II).

4. With regard to the title,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the drawings to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

2

☐ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 99/01494

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07F19/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 592 375 A (SALMON BARDWELL C ET AL) 7 January 1997 (1997-01-07)	1, 3, 16
Y	abstract	6
	column 1 - column 3	
	column 9, line 34 - line 35	
A	claim 1	4, 7, 10, 13
X	EP 0 854 462 A (HITACHI LTD) 22 July 1998 (1998-07-22)	1, 16
Y	abstract	2, 17
	column 1, paragraph 2	
	column 5, paragraph 1	
A	column 6, line 49 - column 7, line 3	5-7, 10, 13
	— -/-	



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"B" document member of the same patent family

Date of the actual completion of the international search

16 November 1999

Date of mailing of the international search report

30/11/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Wolles, B

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	O'MAHONY D.; PEIRCE M.; TEWARI HITESH.: "Electronic Payment System" 1997, ARTECH HOUSE COMPUTER SCIENCE, BOSTON MA XP002122732 23662	6, 17
A	Chapter 4, section 9: Secure Electronic Transactions	9, 12, 15
Y	EP 0 822 535 A (AT & T CORP) 4 February 1998 (1998-02-04)	6
A	abstract column 1, paragraph 1 column 1, line 50 - line 54 column 4, line 3 - line 16 column 5, paragraph 1 column 6, line 23 - line 30 column 9, line 38 - column 10, line 9 column 10, line 34 - column 11, line 13 claim 13	1, 4, 7, 8, 11, 14
Y	EP 0 370 146 A (STRATEGIC PROCESSING CORP) 30 May 1990 (1990-05-30) abstract column 2, line 20 - line 34 column 8, line 45 - line 48	2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB 99/01494

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5592375	A	07-01-1997	AU 1996695 A WO 9524687 A	25-09-1995 14-09-1995
EP 0854462	A	22-07-1998	JP 10149394 A CA 2221399 A	02-06-1998 21-05-1998
EP 0822535	A	04-02-1998	CA 2210281 A	01-02-1998
EP 0370146	A	30-05-1990	US 4799156 A CA 1281417 A	17-01-1989 12-03-1991



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ :

G07F 19/00, G06F 17/60

A1

(11) International Publication Number:

WO 00/17834

(43) International Publication Date:

30 March 2000 (30.03.00)

(21) International Application Number: PCT/IB99/01494

(22) International Filing Date: 2 September 1999 (02.09.99)

(30) Priority Data:

98117856.9

21 September 1998 (21.09.98)

EP

(71) Applicant (for all designated States except US): INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armon, NY 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): ABAD PEIRO, Jose L. [ES/FR]; La Gonette, F-38450 St. Georges de Commiers (FR). STOLZE, Markus [DE/CH]; Zopfstrasse 15, CH-8134 Adliswil (CH).

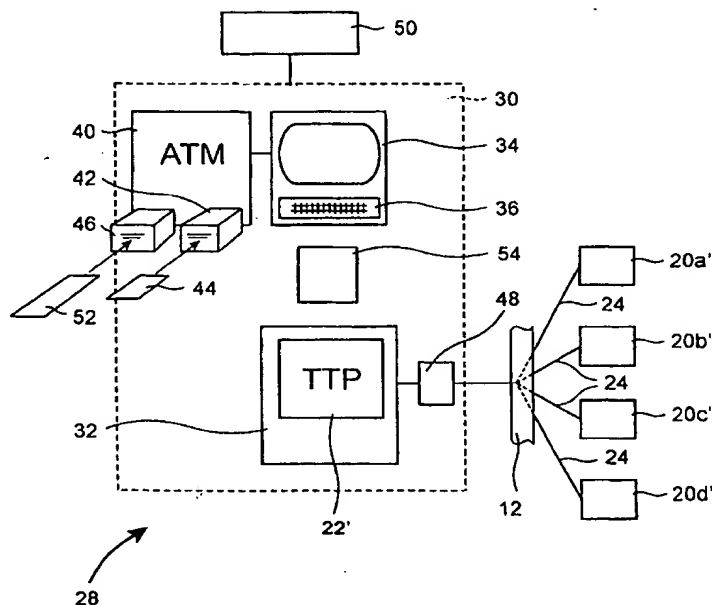
(74) Agent: KLETT, Peter, Michael; International Business Machines Corporation, Saeumerstrasse 4, CH-8803 Rueschlikon (CH).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: METHOD OF IMPROVING SECURITY IN ELECTRONIC TRANSACTIONS



(57) Abstract

A computerized method (10) is provided which improves data security in electronic transactions in an insecure network (12). This is accomplished when the method (10) operates on a user (18) which has established a commercial relationship with a trusted third party broker (22), and merchants (20a - 20d). The method utilizes network links (14, 24) between (a) the trusted third party broker and the user and (b) the trusted third party broker and the merchants. Protocols are selected to operate between each network link, the selection being made, at least in part, on the basis of the computer resources which may be expected to be available in each network link.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 99/01494

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 G07F19/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 592 375 A (SALMON BARDWELL C ET AL) 7 January 1997 (1997-01-07)	1,3,16
Y	abstract	6
	column 1 -column 3	
	column 9, line 34 - line 35	
A	claim 1	4,7,10, 13
X	EP 0 854 462 A (HITACHI LTD) 22 July 1998 (1998-07-22)	1,16
Y	abstract	2,17
	column 1, paragraph 2	
	column 5, paragraph 1	
A	column 6, line 49 -column 7, line 3	5-7,10, 13
	— -/-	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

16 November 1999

Date of mailing of the international search report

30/11/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3018

Authorized officer

Wolles, B

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 99/01494

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	O'MAHONY D.; PEIRCE M.; TEWARI HITESH.: "Electronic Payment System" 1997, ARTECH HOUSE COMPUTER SCIENCE, BOSTON MA XP002122732 23662	6, 17
A	Chapter 4, section 9: Secure Electronic Transactions	9, 12, 15
Y	EP 0 822 535 A (AT & T CORP) 4 February 1998 (1998-02-04)	6
A	abstract column 1, paragraph 1 column 1, line 50 - line 54 column 4, line 3 - line 16 column 5, paragraph 1 column 6, line 23 - line 30 column 9, line 38 - column 10, line 9 column 10, line 34 - column 11, line 13 claim 13	1, 4, 7, 8, 11, 14
Y	EP 0 370 146 A (STRATEGIC PROCESSING CORP) 30 May 1990 (1990-05-30) abstract column 2, line 20 - line 34 column 8, line 45 - line 48	2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB 99/01494

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5592375 A	07-01-1997	AU 1996695 A WO 9524687 A	25-09-1995 14-09-1995
EP 0854462 A	22-07-1998	JP 10149394 A CA 2221399 A	02-06-1998 21-05-1998
EP 0822535 A	04-02-1998	CA 2210281 A	01-02-1998
EP 0370146 A	30-05-1990	US 4799156 A CA 1281417 A	17-01-1989 12-03-1991

is to provide confidentiality of information, ensure payment integrity, and authenticate both merchants and cardholders. The current computing requirements for implementing the SET protocol make it inappropriate as a protocol for shopper/users to run directly from their browser. If such were used by the user, for example, in
5 downloading an applet, downloading times and performance losses would likely increase to unacceptable levels.

Further, unless the user has some mechanism of fair exchange, the user must trust the merchant, an entity with whom the user may not have had dealings and about
10 which he is only able to obtain information from the merchant himself. The justifiable lack of trust in a merchant-server's self certification (e.g., the fear of merchant fraud) tends to limit the growth and acceptability of electronic commerce. Therefore, even when organizations use the SET protocol to perform payment functions, the user's lack of anonymity is a disadvantage.

15 The prior art describes various attempts at improving security. These attempted solutions fall into two categories: (1) third party protocols which make use of a trusted, on-line third party who is typically registered as such by a neutral entity, and (2) gradual exchange protocols in which the probability of obtaining a fair exchange is
20 gradually increased over several rounds of communications. In common commercial terms, this latter protocol is comparable to a "course of dealing" between the parties involved in the exchange. In the trusted third party approach, organizations managing a trusted third party must conform to a number of requirements. For example, a trusted third party may be required to (1) meet minimum financial criteria, (2) to possess
25 insurance against fraud, and (3) be socially credible. Proper adherence to and implementation of these requirements ensures that information disclosed by users to a trusted third party is handled in a secure manner.

These two prior art solutions have shortcomings. For example, the third party
30 method runs the risk of the third party becoming a bottleneck due to the fact that a

Claims

1. A computerized method of transacting electronic commerce in an insecure
5 network, the method improving data security in the insecure network by:
 - a. operating on and between a user which has established a commercial relationship with a trusted third party, and merchants; and
 - b. utilizing:
 - i. network links between:
10 (1) the user and the trusted third party broker and
(2) the trusted third party broker and the merchants; and
 - ii. protocols which operate on each network link, selected, at least in part, on the basis of the computer resources which may be expected to be available in each network link.
- 15 2. The method of claim 1 wherein a server of the trusted third party is built into a housing which includes a terminal interface thus permitting users to select and purchase the insurance products of insurance companies at a remote site such as at an airport.
- 20 3. The method of claim 1 wherein the trusted third party broker is an employment consultant certified as a trusted third party, the merchants are companies seeking employees, and the users are persons seeking employment.
- 25 4. The computerized method of claim 1 comprising:
 - a. permitting the user, using a browser and a low resource-intensive secure communication protocol, to access the trusted third party broker in order to request broker services;
 - b. the trusted third party broker gathering information from web servers of
30 the merchants which offer competitive products which may satisfy the user's request;

- c. the browser presenting an interactive window to the user which allows the user to compare differences between the competitive products and choose between the competitive products;
 - d. the user choosing between the competitive products, thus selecting a merchant and issuing a payment order through the trusted third party broker for the benefit of the merchant;
 - e. the trusted third party broker transmitting the payment order to the merchant using a highly secure payment protocol, thus paying the merchant on behalf of the user; and
 - f. the merchant and a bank cooperating using a highly secure payment protocol enabling the merchant to receive payment from the bank.
- 5.
- The computerized method of claim 4 additionally comprising providing confirmation of payment on the payment order to the user.
- 6.
- The computerized method of claim 4 wherein the low resource-intensive secure communication protocol is the SSL protocol, the highly secure payment protocol is the SET protocol, the browser is JAVA-enabled, and the interactive window is an applet.
- 7.
- A computerized method of enabling a trusted third party broker, interfacing with users on an insecure network, to offer users the ability to browse, compare, and purchase using secure payment facilities irrespective of the level of security in communications between the user and the trusted broker, the method comprising :
- a. using a low resource-intensive secure communication protocol, presenting a user with an interface from which the user can browse, request information concerning the products of merchants, and compare such information via an interactive window;
 - b. gathering the requested information from merchants;

- c. using a low resource-intensive protocol, providing the requested information to the user via an interactive window;
 - d. upon the user's selection of a product offered by a merchant, receiving the user's payment order;
 - 5 e. using a highly secure payment protocol, transmitting the payment order to a selected merchant who may then receive payment thereon, and, subsequently, transmit confirmation of payment thereon to the trusted broker; and
 - f. transmitting confirmation of payment to the user.
- 10
- 8. The computerized method of claim 7 wherein the user browses using a browser which is JAVA-enabled, and the interactive window is an applet.
 - 9. The computerized method of claim 7 wherein the low resource-intensive secure
 - 15 communication protocol is the SSL protocol and the highly secure payment protocol is the SET protocol.
- 20
- 10. A computerized method enabling a user to browse, compare, and purchase products offered by merchants using secure payment facilities irrespective of the available level of security in communications between the user and the merchant, the method comprising:
 - a. using a low resource-intensive secure communication protocol, transmitting requests for information concerning the products of interest provided by the merchants to a trusted third party broker;
 - 25 b. receiving such information via an interactive window configured by the trusted broker;
 - c. upon the user's selection of a product offered by a merchant, creating a payment order which is transmitted to the merchant by the trusted broker using a highly secure payment protocol, the selected merchant
 - 30 then receiving payment thereon; and
 - d. receiving confirmation of payment.

11. The computerized method of claim 10 wherein the user browses using a browser which is JAVA-enabled, and the interactive window is an applet.
- 5 12. The computerized method of claim 10 wherein the low resource-intensive secure communication protocol is the SSL protocol and the highly secure payment protocol is the SET protocol.
- 10 13. A computerized method enabling a merchant to offer products in a forum in which users may browse, compare the features of the merchant's products with products offered by other merchants and purchase such products using secure payment facilities irrespective of the security in communications between the user and the merchant, the method comprising:
- 15 a. receiving a request from a trusted third party broker for information;
- b. providing product information through an interactive window over a network to the third party broker;
- c. using a highly secure payment protocol, receiving a payment order through the third party broker from the user;
- d. using a highly secure payment protocol, obtaining payment on the payment order; and
- 20 e. transmitting confirmation of receipt of payment to the third party broker who may in turn provide confirmation to the user.
14. The computerized method of claim 13 wherein the user browses using a browser which is JAVA-enabled, and the interactive window is an applet.
- 25 15. The computerized method of claim 13 wherein the low resource-intensive secure communication protocol is the SSL protocol and the highly secure payment protocol is the SET protocol.

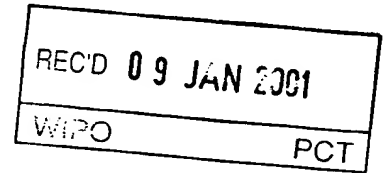
16. A computer-readable medium encoded with a computerized method of transacting electronic commerce in an insecure network, the method improving data security in the insecure network by:
- a. operating on and between a user, which has established a commercial relationship with a trusted third party broker, and merchants; and
 - b. utilizing:
 - i. network links between:
 - (1) the user and the trusted third party broker and
 - (2) the trusted third party broker and the merchants; and
 - ii. protocols which operate on the network links, selected, at least in part, on the basis of the computer resources which may be expected to be available in each network link.
17. The method of claim 16 wherein the network link between the user and the trusted third party broker uses a low resource-intensive secure communication protocol such as the SSL protocol and the network link between the third party broker and the merchant uses a highly secure payment protocol such as the SET protocol

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)



Applicant's or agent's file reference SZ9-98-004	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB99/01494	International filing date (day/month/year) 02/09/1999	Priority date (day/month/year) 21/09/1998
International Patent Classification (IPC) or national classification and IPC G07F19/00		
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.


2. This REPORT consists of a total of 9 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 11/03/2000	Date of completion of this report 05.01.01
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Stratford, C Telephone No. +49 89 2399 2268



INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/IB99/01494

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).):*

Description, pages:

1,3-17	as originally filed	
2,2a	with telefax of	06/10/2000

Claims, No.:

1-17	as received on	04/12/2000	with letter of	30/11/2000
------	----------------	------------	----------------	------------

Drawings, sheets:

1/8-8/8	as originally filed
---------	---------------------

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/IB99/01494

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

5. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

see separate sheet

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims 1-17
	No:	Claims
Inventive step (IS)	Yes:	Claims
	No:	Claims 1-17
Industrial applicability (IA)	Yes:	Claims 1-17
	No:	Claims

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

1.0 With reference to Section I

- 1.1 The phrase 'whereby the reduced security ... issued by a certification authority' added to claims 1, 7, 10, 13, and 16 with the amendments received on 4.12.00 falls beyond the scope of the original disclosure, as forbidden by Article 34(2)(b) PCT. It states that the security of the communication protocol is improved by the trust given to the third party. However, this trust has no influence on the security of the protocol itself, rather on the security of the transaction as a whole. There is no basis in the original application for this (incorrect) statement, and as such the claims have been examined as if this phrase had not been added (as required by Rule 66.4*bis* PCT).
- 1.2 However, even if this phrase stated that the overall security is improved, it could still not be considered to be inventive. Every trusted third party will in practice need credentials of some form to guarantee its trustworthiness - the use of a certificate by a certification authority is a common choice for electronic applications.

5.0 With reference to Section V

- 5.1 Reference is made to the following documents:-

- D1: US-A-5 592 375 (SALMON BARDWELL C ET AL) 7 January 1997
(1997-01-07)
- D2: EP-A-0 854 462 (HITACHI LTD) 22 July 1998 (1998-07-22)
- D3: O'MAHONY D.; PEIRCE M.; TEWARI HITESH.: 'Electronic Payment System'
1997, ARTECH HOUSE COMPUTER SCIENCE, BOSTON MA
XP002122732 23662
- D4: EP-A-0 822 535 (AT & T CORP) 4 February 1998 (1998-02-04)

This numbering will be adhered to throughout the application process.

- 5.2 Independent claims 1 and 16 fail to meet the requirements of Article 33(3) PCT because they lack an inventive step.

The document D1 (in particular Figure 1) is regarded as being the closest prior art to the subject-matter of these claims, and discloses (the references in parentheses applying to this document):

A computerised method of transacting electronic commerce in an insecure network (see Abstract), the method improving data security in the insecure network by:

- (a) operating on and between a user ('Buyer') which has established a commercial relationship with a certified trusted third party ('Server', see column 13, lines 61-62), and merchants ('Seller');
- (b) utilising a network link between the user and the third party and a network link between the third party and the merchants (column 14, lines 20- 34); and
- (c) utilizing a communication protocol which operates on the network link between the user and the third party (obviously present); and
- (d) utilizing a payment protocol, which is more resource intensive than the communication protocol, which operates on the network link between the third party and the merchants (column 1, lines 50-55, in the likely case where both interfaces have two modes, the user has a low-bandwidth communications channel, and the merchant a high-bandwidth communications channel. The fact that two modes are specifically disclosed indicates clearly that there are different protocols involved, and not simply one protocol operating faster or slower).

Thus the only difference between claim 1 and D1 is that D1 does not state that the high resource intensive protocol is more secure. However, the skilled person will clearly want as much security as is reasonably possible due to the sensitive information being transferred. With the means already in place for choosing the protocol depending on available bandwidth, it would be obvious to implement higher security in the second mode protocol where it is known that a higher bandwidth is available.

Therefore claim 1 is not inventive. Claim 16, as the corresponding computerised method, is similarly not inventive.

5.3 Independent claim 7 also fails to meet the requirements of Article 33(3) PCT

because it lacks an inventive step. Document D1 (in particular Figures 1 and 5) discloses:

A computerised method of enabling a trusted third party (Figure 1, 'Server'), interfacing with users ('Buyers') on an insecure network (column 14, lines 20-34), to offer users the ability to browse and compare information (column 1, lines 19-25) and purchase products, (see column 13, lines 65-67, and Figure 5, steps 570 and 572), the method comprising:

- (a) using a communication protocol (necessarily present), presenting a user with an interface from which the user can browse and request information concerning the products of merchants ('Sellers', column 3, lines 14-24), and compare such information via an interactive window;
- (b) gathering the requested information from the merchants;
- (c) using the communication protocol, providing the requested information to the user via the interactive window (see Figure 5, also column 2, lines 11-14 and column 3, lines 38-47).

This follows partially the wording of claim 7, with the exception that details of the payment procedure are not explained in D1, hence the following features are not disclosed therein:-

- (i) that payment is by means of a secure payment facility, irrespective of the level of security between the user (buyer) and the third party
- (ii) that upon the user's selection of a product offered by a merchant (seller), the user's payment order is received;
- (iii) that payment is transmitted by means of a payment protocol, which is more secure than the communication protocol;
- (iv) that confirmation of payment is transmitted to the third party; and
- (v) that confirmation of payment is transmitted to the user.

As it is not even clear from D1 if the payments themselves are carried out over the network, none of the above can be assumed to be the case. However, D2, which describes a system for purchasing products/services over the Internet, does go into more detail concerning how the online payments are carried out. It discloses:

- (i) that payment is by means of a secure payment facility (the 'electronic cash'

- described in column 1 of D2 clearly has its own security features),
- (ii) that upon the user's (buyer's) selection of a product offered by a merchant (prospective employee), the user's payment order is received (see column 6, lines 35-40);
 - (iii) that payment is transmitted by means of a highly secure payment protocol, upon receipt of which the merchant may receive payment (Figure 5, step 6007, whereby the settlement message, containing the (secure) payment, is transmitted to the merchant; see also column 7, lines 16-20);

There is no mention of the transmission of receipts of payment, merely those of receipts of goods purchased. However, acknowledging payment with a receipt is standard practice, whether carried out on paper or electronically.

Consequently, the skilled person, when wishing to e.g. add online payment facilities to the device of D1, would clearly consider incorporating the techniques described in D2 (i.e. i-iii) to the method known from D1, without the use of any inventive activity. Due to the two independent protocols of D1 (column 1, lines 50-55), this would automatically result in using secure payment facilities (between the merchant and the third party) which are irrespective of the available level of security between the user and the third party. Adding the provision of payment receipts is an obvious option available to the skilled person, which is also not inventive.

- 5.4 Independent claims 10 and 13 fail to meet the requirements of Article 33(3) PCT because they lack an inventive step.

The features of these claims correspond to those of claim 7, simply seen from a different perspective, i.e. that of the user and merchant respectively. However, in essence they are the same features, and so are similarly preempted by documents D1 and D2.

- 5.5 Dependent claims 2-6, 8-9, 11-12, 14-15 and 17 also fail to meet the requirements of Article 33(3) PCT because they lack an inventive step. The detailed reasoning therefore is given below.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB99/01494

5.6 With reference to claim 2, the fact that the trusted third party of D1 is a server (see Figure 1), implies that it is built into a housing including a terminal interface. The use of D1's system for selling products is suggested (column 2, line 20), and choosing a specific type of product, for example insurance (which does not necessarily require the transfer of a physical entity), which is suitable for online commerce does not amount to an inventive step.

5.7 The features of claim 3 are clearly present in D1 (column 3, lines 28-36; obviously the names 'merchants' and 'users' are arbitrary, and can be interchanged).

5.8 With reference to claims 4 and 5, D1 discloses the following points, references for which are given:-

- | | |
|-----------------------------|--|
| (1) and (3) | column 3, lines 37-47, and column 9, lines 30-35 |
| (2) | Figure 1, and column 3, lines 19-21 |
| (4) (without payment order) | Figure 5, step 570 |

The references to payment, part of (4), (5) and (6) are not disclosed in D1, but are known from D2 (see Section 5.3).

5.9 Claims 6, 8-9, 11-12, 14-15, and 17 specify the communication protocol and the payment protocol as being the SSL and SET protocols respectively, that the browser is JAVA enabled, and that the interactive window is an applet.

SSL and SET protocols are industry standards, with well known advantages and disadvantages (e.g. level of security offered, processing time required, level of anonymity, etc.). Depending on the exact requirements, these two protocols represent the obvious choices for payment protocols (see D3 for reference).

Similarly, the use of JAVA browsers and applets is also known as a means of providing interactivity over the Internet (see for example, D4, column 6, lines 23-30).

5.10 It should be noted that the terms 'such as' (claims 2 and 17) and 'may' (claims 4, 7, and 13) indicate that the following feature is optional, and could be ignored for the purposes of examination.

5.11 The industrial applicability of all of the claims is self-evident, thus complying with the requirements of Article 33(4) PCT.

7.0 With reference to Section VII

7.1 Figure 1 is incorrectly described (on page 5) as a 'computerised method' (ref. 10), while it is clearly showing a network system. Figure 3 correctly shows the method. Furthermore, the same reference number cannot be used to show two different entities (i.e. a method and a system).

8.0 With reference to Section VIII

8.1 Claims 10 and 13 are unclear (Article 6 PCT) because they state that secure payment facilities can be used irrespective of the available level of security in communications between the user and the merchant. This is clearly not the case; the security is irrespective of the communications between the user and the third party.